

Browser und Erweiterungen

Wahl des Browsers

Empfohlener Webbrowser: **Mozilla Firefox** (ab Version 57)

- Für GNU/Linux, Windows und macOS: <https://mozilla.org/de/firefox/new/>
- Für Android: <https://www.mozilla.org/de/firefox/android/>
- Für iOS: <https://www.mozilla.org/de/firefox/ios/>

Einstellungen

≡ **Menübutton** → *Einstellungen* → *Datenschutz & Sicherheit*:

- **Chronik**: nach benutzerdefinierten Einstellungen, dort z.B. einstellen:
 - Cookies von Drittanbietern akzeptieren: Nie
 - Chronik löschen, wenn Firefox geschlossen wird (insbes. Cookies)
 - Schutz vor Aktivitätenverfolgung: Immer
 - **Do Not Track** aktivieren (Websites mitteilen, Ihre Aktivitäten nicht zu verfolgen)

≡ **Menübutton** → *Einstellungen* → *Suche*:

- Alternative **Suchmaschinen** hinzufügen, Suchvorschläge deaktivieren und Standardsuchmaschine ändern (z.B. StartPage.com, Ixquick.eu, MetaGer.de, DuckDuckGo.com)

Erweiterungen / Add-ons & Plugins

≡ **Menübutton** → *Add-ons* → *Erweiterungen* → *Alle Add-ons durchsuchen*:

- **uBlock Origin** blockiert Werbung und Tracker
- **HTTPS Everywhere** ruft verschlüsselte Verbindung zu Websites auf, wenn verfügbar
- **NoScript** verbessert die Sicherheit des Browsers und blockiert die Ausführung von Programmen – Add-on-Einstellung: *Scripts Globally Allowed* (auch wenn dies vom Entwickler nicht empfohlen wird)
- **Cookie AutoDelete** löscht Cookies automatisch nach dem Schließen von Browserfenstern und -tabs

Add-ons für Fortgeschrittene:

- **NoScript** mit der Standardeinstellung, also nicht *Scripts Globally Allowed*; Außerdem: Whitelist bereinigen
- **uMatrix** unterbindet alle Drittanbieteraufrufe

Adobe Flash Player:

- Deinstallieren oder Deaktivieren (**Shockwave Flash** unter **Add-ons** → **Plugins**)
- Falls man auf Flash angewiesen ist: Nur auf Nachfrage aktivieren

Wirkung der Einstellungen und Add-ons überprüfen:

- Die Erweiterung **Lightbeam** zeigt von welchen Drittanbietern Inhalte nachgeladen werden (eine dauerhafte Aktivierung des Add-ons ist nicht ratsam, da es langsam ist)
- Ohne Add-on: ≡ **Menübutton** → **Web-Entwickler** → **Netzwerkanalyse** zeigt beim Laden einer Website alle Anfragen als Liste
- Der Browser-Fingerabdruck testen: <https://panopticklick.eff.org/>

Passwörter

Passwörter (wenn möglich) nicht im Firefox speichern. Für alle gängigen Betriebssysteme gibt es den Passwortmanager KeePassX: <https://www.keepassx.org/>

Tor-Browser

Der Tor-Browser ist ein vorkonfigurierter Firefox, der über das Tor-Netzwerk im Internet surft – Erweiterungen zum Schutz der Privatsphäre sind bereits installiert. Weitere Informationen und Download unter: <https://www.torproject.org/>

Bitte beachtet die umfangreiche Dokumentation, da eure Anonymität im Tor-Netzwerk vor allen Dingen von eurem Surf-Verhalten abhängt. Installiert **keine weiteren Add-ons** und lest vor Benutzung die offizielle Dokumentation:

<https://www.torproject.org/docs/documentation.html.en> (Englisch)